AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Benjamin P Paris, being first duly sworn under oath and deposed, state the following:

INTRODUCTION

1. I make this affidavit in support of an application for a warrant to search a black SOYES cell phone, approximately 4 inches in length, 1 inch in width, and a sim card, both currently located in the FBI Philadelphia Division's evidence control room at 600 Arch Street, Philadelphia, Pennsylvania (hereinafter, the "Subject Devices") as described in Attachment A, which was found following a routine search of an inmate at the Federal Detention Center (FDC) in Philadelphia and is believed to contain evidence relevant to an investigation into the introduction of contraband into the FDC on September 14, 2020, in violation of 18 U.S.C. § 1791(a)(2). Inmates at the FDC are informed upon entry as to what items they are prohibited from having. Additionally they are made aware of the routine searches of their person, cell and personal property while housed at the FDC.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI) assigned to the Philadelphia, Pennsylvania Division. I have been employed with the FBI since July 31, 2011. I am currently assigned to the Violent Crimes Task Force (VCTF) and have been since November 2018. My current duties include, among other things, the investigation of bank robberies, fugitives, kidnappings, Hobbs Act robberies, and crimes committed at the Federal Detention Center in Philadelphia, Pennsylvania. Before becoming a Special Agent with the FBI, I was a sworn police officer in the state of Delaware from February of 2007 until June of 2011.

3. Based on my training and experience and the facts as set forth in this affidavit there is probable cause to believe that GEORGE FELTS, inmate number 69817-066, has committed a violation of 18 U.S.C. 1791(a)(2) (providing or possessing contraband in prison). There is also probable cause to search the information described in Attachment A for evidence of these crimes, as described in Attachment B.

PROBABLE CAUSE

4. On September 14, 2020, at approximately 2:35 PM, Federal Detention Center (FDC) staff were conducting rounds on unit 6 South and approached cell 643 where multiple inmates were observed in the cell, including FELTS. Upon noticing the FDC staff approaching, the inmates began to disperse and ignored commands to stop so that pat searches of the inmates could be conducted. FELTS began to run from FDC staff along the top tier of the unit and a Correctional Officer (CO) gave chase. As FELTS approached the CO's office on the tier, he reached into his pocket and handed a black SOYES cell phone to an inmate who was standing in the area. As FELTS was taken into custody by other COs in the vicinity, the original CO who pursued FELTS recovered the phone from the hands of the inmate to whom FELTS passed it.

5. During the month of October 2020, FDC staff received information from another inmate that FELTS had kept an unknown quantity of drugs in his cell prior to being moved to the Special Housing Unit (SHU) for the incident described in paragraph four above. FELTS' cell was searched at the time of his re-assignment to the SHU, although the tops of pill bottles containing vitamins and allergy medication were not thoroughly examined. The property from his cell was then packaged within an individual storage container and stored in the secure Property Office within the SHU. Only FDC staff assigned to that Property Office had access to

the items within including FELTS' property. Based upon the information from the inmate, FDC staff conducted a second search of FELTS' property. In particular, the tops of pill bottles were removed and examined. As a result of this, approximately 249 strips of Suboxone and a cellular phone SIM card were discovered.

6. I know from my training and experience in investigating crimes that occur within the FDC, and from speaking with employees of he Federal Bureau of Prisons that work at the FDC, that inmates are prohibited from possessing cell phones within the FDC. Additionally, I am aware that inmates are not permitted to possess Suboxone, a controlled substance, within the FDC. As a result I know that both types of items seized from FELTS and his property, the Suboxone, the cell phone, and the cell phone SIM card, are contraband for inmates in the FDC.

7. I know from my experience in investigating crimes committed by inmates at the FDC that cell phones are utilized by inmates to contact individuals outside the FDC to further criminal activity both within the FDC and outside. This writer and other special agents in the Philadelphia Division of the FBI are currently investigating numerous other incidents in which an inmate at the FDC utilized a cell phone from within the facility either to arrange for contraband to be brought by someone during a visit to the FDC or through holes made in cell windows and attached to ropes that were lowered from the window.

CONCLUSION

8. The Subject Telephone is a wireless telephone. Based on my training and experience, as well as the training and experience of other agents, a wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used primarily for voice communication through radio signals. These telephones send signals through networks of transmitter/receivers called "cells," enabling communication with other wireless telephones or

traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include, but are not limited to: storing names and phone numbers in electronic "address books;" sending, receiving, and storing email, voice messages and text messages; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the internet. Wireless telephones may also include global positioning system (GPS) technology for determining the location of the device and for mapping and navigation features. Based on my training and experience, I am aware that people who engage in illegal activities such as robberies have been known to use some or all of these features in the furtherance of their illegal activities.

9. Furthermore, based on my training and experience, I know that electronic devices such as cell phones can store information for long periods of time. Even when a user deletes information from a device, it can sometimes be recovered with forensic tools. Similarly, things that have been viewed via the internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensic tools.

10. This application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the device because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a device is evidence may depend on other information stored on the device and the application of knowledge about how a device behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

11. Searching for the evidence described in Attachment B may require a range of data analysis techniques. In some cases, agents and computer analysts may be able to conduct carefully targeted searches that can locate evidence without requiring a time consuming manual search through unrelated materials that may be commingled with criminal evidence. In other cases, however, such techniques may not yield the evidence described in the warrant. Criminals can mislabel or hide information, encode communications to avoid using key words, attempt to delete information to evade detection, or take other steps designed to frustrate law enforcement searches for information. These steps may require agents and law enforcement or other analysts with appropriate expertise to conduct more extensive searches, such as scanning storage areas unrelated to things described in Attachment B, or perusing all stored information briefly to determine whether it falls within the scope of the warrant. In light of these difficulties, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant I am applying for would permit the examination of the device using whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

/s FBI Special Agent Benjamin Paris
Benjamin P. Paris
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
this 8th day of December 2020.

s/ Magistrate Judge Richard A. Lloret

Honorable Richard A. Lloret
United States Magistrate Judge

ATTACHMENT A
ITEMS TO BE SEARCHED

A black SOYES cell phone, approximately 4 inches in length, 1 inch in width, currently located at the FBI Philadelphia Division, assigned evidence number 1B3; and a sim card, identifying number 89011410227959296072O, assigned evidence number 1B4.

ATTACHMENT B
ITEMS TO BE SEIZED

1. All records that relate to violations of 18 U.S.C. § 1791(a)(2)(providing or possessing contraband in prison), including:

    a. Documents in electronic form, including correspondence, records, opened or unopened emails, text messages, voicemail messages, call logs, chat logs, internet history.

2. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including, but not limited to the following:

    a. Forms of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

    b. Data that has been manually programmed into a GPS navigation system, as well as data automatically stored by the GPS navigation system, including any and all electronic data which can be collected, analyzed, created, displayed, converted, stored, concealed, or transmitted, or similar computer impulses or data.

    c. Stored electronic information and communications, including but not limited to, telephone or address directory entries consisting of names, addresses and

telephone numbers; logs of telephone numbers dialed, telephone numbers of missed calls, and telephone numbers of incoming calls; schedule entries; stored memoranda; stored text messages; stored photographs; store audio; and stored video.

3. Evidence and contents of logs and files on the device, such as those generated by the device's operating system, which describes the history and use of the device, including but not limited to files indicating when files were written, were opened, were saved, or were deleted. Evidence tending to show the identity of the person using the device at the time any actions relating to the above offenses were taken.